



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/581,332	08/28/2000	Sylvain Chevreau	RCA90215	4067

7590 12/18/2003  
Joseph S Tripoli  
Thomson Multimedia Licensing Inc  
CN 5312  
Princeton, NJ 08543-0028

EXAMINER

KIM, CHONG R

ART UNIT	PAPER NUMBER
----------	--------------

2623

DATE MAILED: 12/18/2003

10

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

09/581,332

Applicant(s)

CHEVREAU ET AL.

Examiner

Charles Kim

Art Unit

2623

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 22 September 2003.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 9-16 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 9-16 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 28 August 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. §§ 119 and 120

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☒ All b) ☐ Some \* c) ☐ None of:  
1. ☐ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. ☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).  
\* See the attached detailed Office action for a list of the certified copies not received.
- 13) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.  
a) ☐ The translation of the foreign language provisional application has been received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892) 4) ☐ Interview Summary (PTO-413) Paper No(s). \_\_\_\_\_
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) 5) ☐ Notice of Informal Patent Application (PTO-152)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) \_\_\_\_\_. 6) ☐ Other: \_\_\_\_\_

## **DETAILED ACTION**

### ***Response to Amendment and Arguments***

1. Applicant's amendment filed on September 22, 2003 has been entered and made of record.
2. Applicant's substitute specification filed on September 22, 2003 has been entered and made of record. The Examiner notes that there appears to be no new matter in the substitute specification. The applicants admit (page 13) that they mistakenly transposed the terms "encrypt" and "decrypt" in the specification. The specification has been replaced by the substitute specification in order to correct what appears to be an obvious error.
3. In view of applicant's cancellation of the claims in the amendment, the objection to the claims 4, 5, and 8 are withdrawn.
4. In view of applicant's amendment, the 112 first paragraph rejections are withdrawn.

### ***Claim Objections***

5. Claims 9-16 are objected to because of the following informalities: typographical errors. There appears to be a typographical error in the phrase "detectable element" in line 5 of claim 9. It appears that the applicant intended the phrase to read "detachable element". Appropriate correction is required.

### ***Claim Rejections - 35 USC § 112***

The following is a quotation of the second paragraph of 35 U.S.C. 112:

Art Unit: 2623

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 12 and 13 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Referring to claim 12, the phrase "the chip card" in line 3 lacks antecedent basis. For examination purposes, the phrase "the circuit associated with the secret key K1 of the chip card carrying out processing" in lines 3-4 will be interpreted as "the circuit associated with the secret key K1 carrying out processing". Appropriate correction is required.

Referring to claim 13, the phrase "the chip card" lacks antecedent basis. It appears that the applicant intended the phrase to read "a chip card". Appropriate correction is required.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 9-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Friedman U.S. Patent No. 5,499,294 ("Friedman") and Vu et al., U.S. Patent No. 6,557,104 ("Vu").

Art Unit: 2623

Referring to claim 9, Friedman discloses a device for authenticating the taking of pictures made up of digital data comprising a picture taking apparatus (11) and a security element (12) carrying out the signing of at least part of the digital data, wherein the security element is an element comprising a circuit associated with a secret (unique private) key K1 giving output digital data which are a signature of digital data at the input (col. 5, lines 49-65).

Friedman fails to explicitly disclose that the security element is a detachable element, and the detachable element and the associated secret key K1 are specific to a user. However, this feature was exceedingly well known in the art. For example, Vu discloses a detachable security element (smart card) comprising a circuit associated with a secret key for signing digital data; the detachable element and the associated secret key being specific to a user (col. 1, lines 34-39 and lines 58-67).

Friedman and Vu are both concerned with authentication systems that utilize secret keys for encrypting digital data. Friedman is concerned with protecting the secret key from being exposed to unauthorized users (Friedman, col. 3, lines 9-15). Vu's detachable security element (smart card) provides a secured environment for storage and processing of the secret key because all operations based on the secret key are performed within its boundary, and therefore prevents the secret key from being exposed to the outside world (Vu, col. 2, lines 11-15). Therefore, it would have been obvious to modify the security element of Friedman, so that it is a detachable security element as taught by Vu, in order to enhance the security of the authentication system.

Friedman and Vu both fail to explicitly disclose that the detachable element connects up to the picture taking apparatus by an interface circuit provided in the picture taking apparatus. However, Vu states that "any application which requires some secret information in order to

process data can be adapted to take advantage of a smart card's secure processing environment" (Vu, col. 2, lines 19-22). In this case, Friedman's application requires some secret information (secret key) to process (sign) data. Therefore, it would have been obvious to modify the picture taking apparatus of Friedman to include an interface circuit, so that it is adapted to take advantage of the secure processing environment provided by Vu's smart card.

Referring to claim 10, Friedman further discloses that the security element incorporates a hashing circuit (12A) [col. 5, lines 56-65 and figure 3B]. As noted above, Vu discloses a detachable security element. Therefore, the combination of Friedman and Vu disclose a detachable element that incorporates a hashing circuit.

Referring to claim 11, Vu further discloses that the detachable element is a chip card (col. 1, line 64-col. 2, line 10).

Referring to claim 12 as best understood, Friedman further discloses that the picture taking apparatus comprises a multiplexing circuit (12C) and a circuit (12A) for hashing at least one first fraction of the digital data in such a way as to generate a first hashed datum, the circuit associated with the secret key K1 carrying out the processing of the first hashed datum in such a way as to generate a signature of the first hashed datum (col. 4, lines 33-37 and col. 5, lines 56-63. Note that the block of the image file is interpreted as a first fraction of the digital data), the signature and the digital data being transmitted to the multiplexing circuit so as to constitute a multiplexed signal (col. 8, lines 53-67).

Referring to claim 13 as best understood, see the rejection of at least claims 11 and 12 above. Friedman further discloses that the picture taking apparatus comprises a multiplexing circuit (12C), a security element (12) comprising a hashing circuit (12A) carrying out the

Art Unit: 2623

hashing of at least a first fraction of the digital data originating from the picture taking apparatus in such a way as to generate a first hashed datum, and the first hashed datum is processed in the circuit associated with the secret key K1 in such a way as to generate a signature of the first hashed datum (col. 4, lines 33-37 and col. 5, lines 56-63. Note that the block of the image file is interpreted as a first fraction of the digital data), the signature emanating from the security element and the digital data being transmitted to the multiplexing circuit in such a way as to constitute a multiplexed signal (col. 8, lines 53-67).

Friedman fails to explicitly disclose that the security element is a chip card. However, Vu discloses a detachable security element that is a chip card, as noted above (claim 11). Therefore, it would have been obvious to combine the teachings of Friedman and Vu for the reasons stated above.

Referring to claim 14, Friedman further discloses that the picture taking apparatus (11) is a camera head (col. 5, lines 52-54 and figure 3A).

Referring to claim 15, Friedman further discloses that the picture taking apparatus (11) is a photographic apparatus (col. 5, lines 52-54 and figure 3A).

Referring to claim 16, see the rejection of at least claim 1 above. Friedman further discloses a device (20) for authenticating digital data coming from the device for authenticating the taking of pictures, said device for authenticating the digital data comprising a circuit (22) with public key K2 for calculating a new datum on the basis of the signature, a circuit (21) for hashing at least one second fraction of the digital data in such a way as to generate a second hashed datum, a comparison circuit (23) for comparing the new datum with the second hashed

Art Unit: 2623

datum in such a way as to constitute a signal making it possible to verify the authenticity of the digital data (col. 6, lines 31-52 and figure 3C).

Friedman fails to explicitly disclose a demultiplexer for separating the digital data and the signature. However, Friedman discloses a multiplexing circuit for multiplexing the digital data and the signature at the device for authenticating the taking of pictures (col. 8, lines 53-67). Note that the digital data entering the device (20) will be a multiplexed signal. Friedman also explains that the digital data and the signature are separated prior to being processed by the device (20) [figure 3C. Note that the digital data and the signature are processed separately]. Therefore, the Examiner notes that a demultiplexer is an inherent feature in the device (20) of Friedman, since a multiplexed signal can only be separated if it has been demultiplexed by a demultiplexer.

### *Conclusion*

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,



Art Unit: 2623

however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Dunn et al. U.S. Patent No. 5,987,155 discloses an interface (23) for connecting a detachable element (smart card) to a picture taking apparatus (21).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Charles Kim whose telephone number is 703-306-4038. The examiner can normally be reached on Mon thru Thurs 8:30am to 6pm and alternating Fri 9:30am to 6pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Amelia Au can be reached on 703-308-6604. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-306-0377.

ck

December 11, 2003